NB410: CISCO FIREWALLS MAXIMALE SCORE EN GEMEENTE EPE VERLIEST 600.000 BESTANDEN

Deze week domineerden kritieke kwetsbaarheden en geavanceerde aanvalstechnieken het dreigingslandschap. Een kwetsbaarheid in Cisco firewalls kreeg de maximale dreigingsscore van 10.0 en wordt actief misbruikt voor ransomware, terwijl twee onafhankelijke aanvallen op de toeleveringsketen ontwikkelomgevingen troffen. De aanvalstechniek ClickFix vestigde zich als dominant wapen na een dataroof bij de gemeente Epe waarbij 600.000 bestanden werden gestolen. Een autonome AI agent hackte consultancygigant McKinsey in twee uur en de Europese Unie legde sancties op aan bedrijven achter cyberaanvallen op lidstaten. Dichter bij huis werd een vrouw van 77 in Gilze beroofd door een nepagent en leerden brugklasleerlingen in Breda via het Cyberrijbewijs hoe ze zichzelf online beschermen. Lees alle details in de vijf artikelen van deze week.

CYBERRIJBEWIJS: SCHOLIEREN IN BREDA LEREN ONLINE OVERLEVEN

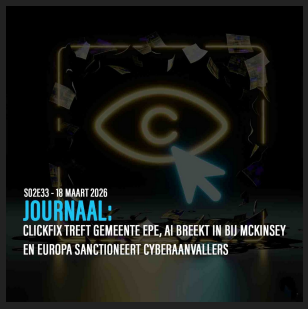
Een op de vijf jongeren wordt slachtoffer van online criminaliteit, maar op school leren ze nauwelijks over de gevaren. Op het Markenhage in Breda volgden brugklasleerlingen de eerste pilot van het Cyberrijbewijs, een interactieve training over phishing, oplichting en sextortion. Hoe een school in Breda het verschil maakt voor de digitale veiligheid van jongeren, ontdek je in dit artikel.

Ontdek hoe het Cyberrijbewijs jongeren beschermt »

CISCO SD-WAN GEHACKT, JUSTITIE GECOMPROMITTEERD EN INTERPOL SLAAT TOE

Een kritieke backdoor in Cisco SD-WAN met de maximale risicoscore wordt al sinds 2023 misbruikt, terwijl de Nederlandse Justitie ICT tweemaal gehackt bleek via een Citrix lek. INTERPOL ontmantelde in een grootscheepse operatie 45.000 malafide servers in 72 landen en Meta schrapt de versleuteling van Instagram berichten. Waarom de Cisco backdoor al drie jaar onopgemerkt bleef, lees je in het journaal.

Bekijk hoe een Cisco backdoor drie jaar lang onopgemerkt bleef »



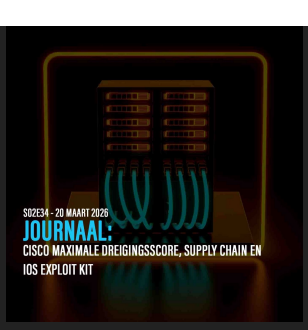
CLICKFIX TREFT GEMEENTE EPE, AI HACKT MCKINSEY, EU SANCTIES

De aanvalstechniek ClickFix vestigde zich als het dominante wapen van cybercriminelen na een grootschalige dataroof bij de gemeente Epe waarbij 600.000 bestanden werden gestolen. Een autonome AI agent hackte consultancygigant McKinsey in twee uur en de Europese Unie legde voor het eerst sancties op aan drie bedrijven achter cyberaanvallen op lidstaten. Hoe een simpele muisklik het begin kan zijn van een complete overname, lees je in het journaal.

Lees hoe ClickFix een hele gemeente lamlegde »

CISCO LEK GEBRUIKT VOOR RANSOMWARE EN AANVAL OP ONTWIKKELAARS

Een kwetsbaarheid in Cisco Secure Firewall Management krijgt de maximale dreigingsscore van 10.0 en wordt actief



misbruikt door de Interlock ransomwaregroep. Tegelijk troffen twee onafhankelijke aanvallen op de toeleveringsketen ontwikkelomgevingen en werd een nieuwe iOS exploit kit met drie zero days ontdekt. Welke van jouw systemen nu al doelwit zijn, ontdek je in het journaal.

Ontdek welke Cisco firewalls nu actief onder vuur liggen »

NEPAGENT STEELT SIERADEN BIJ VROUW VAN 77 IN GILZE

Een vrouw van 77 jaar uit de regio Gilze werd eerst telefonisch opgelicht voor meer dan duizend euro en daarna beroofd van haar sieraden door een man die zich voordeed als politieagent. De politie zoekt getuigen en heeft camerabeelden van de verdachte vrijgegeven. Herken jij deze persoon? Bekijk de beelden en help de politie.

Bekijk de beelden en help de politie »

CYBERCRIME QUIZ WEEK 12 - TEST JE KENNIS!

Weet jij welke Cisco kwetsbaarheid de maximale dreigingsscore van 10.0 kreeg? Hoeveel bestanden verloor de gemeente Epe bij een ClickFix aanval? En in hoeveel uur hackte een AI agent McKinsey? Van backdoors die drie jaar onopgemerkt bleven tot een nepagent die sieraden steelt bij een vrouw van 77.

Test in 20 vragen of jij alles hebt meegekregen!

Liever luisteren of kijken?

Geen tijd om te lezen? Blijf op de hoogte via uw favoriete platform. Kies voor de snelle update, de diepgaande analyse of de visuele presentatie.

Spotify Audio »
DAGELIJKS JOURNAAL (3 min)
DIEPTE ANALYSE (15 min)

YouTube Video »
VISUELE PRESENTATIE (5 min)

Help Cybercrimeinfo in de lucht te houden

Onze tools, journalen en waarschuwingen zijn gratis voor iedereen. Maar onderzoek en hosting kosten geld. Waardeert u onze intelligence? Help ons dan met een eenmalige donatie. Elke bijdrage maakt de digitale wereld een stukje veiliger.

Ik wil graag steunen »

Bedankt voor het lezen! Deel deze nieuwsbrief gerust met vrienden, familie en collega's, samen maken we Nederland en België digitaal weerbaarder.

Tot volgende week,
Cybercrimeinfo